Hardeeville
SOUTH CAROLINA

hardeevillesc.gov
ISSUE 01 | MARCH 2023

TECH TALKS

THE ISSUE

Introduction

Hello everyone! As time slides toward spring, I want to welcome you to our first newsletter from the IT Department at The City of Hardeeville.

IT Security Tips (Do's and Don'ts of online shopping)

Online shopping is convenient and easy, which is why more and more people are turning to this alternative rather than facing the crowds in the stores. . However, there is a dark side to online commerce.

Industry Trends – Q & A

Emerging technologies are arising in the coming years, keep reading to see the top 10 current trends.

NEW YEAR NEW PROJECT

We will be sharing some new information each month about how you can be more aware and take intentional and conscious steps to help minimize your risks while online in this highly transforming digital world. There is so much new technology and trends emerging every day that can impact our lives and transform how we do even the simplest of tasks. While this new technology can be convenient, we still need to take conscious efforts to stay safe and be vigilant in protecting our sensitive information.

What we have for you today: A little article on how how to stay safe while online shopping along with some industry trends and helpful links .

Hardeeville
SOUTH CAROLINA

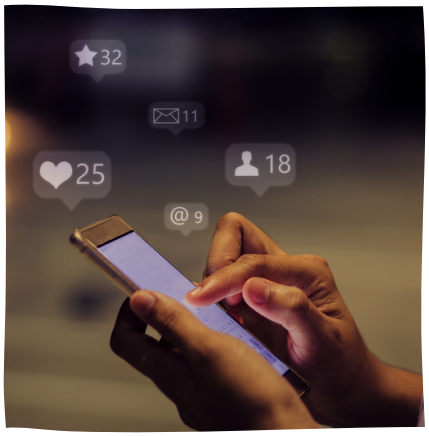
hardeevillesc.gov
ISSUE 01 | MARCH 2023

THE DO'S AND DON'TS OF ONLINE SHOPPING: HOW TO STAY SAFE ONLINE

Online shopping is convenient and easy, which is why more and more people are turning to this alternative rather than facing the crowds in the stores. More than that, you can research items, read reviews and score the best deals. However, there is a dark side to online commerce.

DO – Shop from home. Hackers can easily access public Wi-Fi connections, which means it is safer to make purchases from home than from your favorite coffee shop. Avoid making purchases while connected to airports, hotels or other public hot spots.

DON'T – Social Networking Sites Deals. Do not trust these types of deals, as most URLs are shortened on social media sites. That means you will not know if you are clicking on a legitimate or fraudulent website. You can use these deals as tips but go directly to the retailer's site to check for bargains.



DO – Download an Anti-Phishing Toolbar. If you have not invested in an Anti-Phishing toolbar, consider downloading one. These will help identify fraudulent websites. Many of these toolbars are free.

DON'T – Use your business or personal email addresses. Consider setting up a separate email address for retailers. You can still review any coupons or offers they send you, but it is much easier if this address is hacked than dealing with your business or personal emails.

DO – Select sellers. Most people use a search engine to find a specific item. However, statistics show that approximately three results per search engine page are fraudulent sites looking to steal your personal information. Head directly to retailer's websites or use convenient price-comparison sites. Always check for the https:// in the URL to guarantee your information is transmitted privately. Never make a purchase from a site unless it has an SSL certificate.

ONLINE SHOPPING CONTINUED:

When shopping online, it is better to be safe than sorry, so how to stay safe online. If you follow these helpful tips, you'll greatly decrease your chances of becoming a victim of online fraud. Happy Shopping!

DO – Pay with credit cards. Never use debit card information online. Most of these cards require that fraudulent purchases be reported within two days to obtain the $50 limit liability that is standard with credit cards. If two days pass you by, you can report your loss, but you are limited to 60 days, and your liability is $500. Banks can change these rules, but if possible, use a credit card when making online purchases.

DON'T – Wire money to sellers. Even if you purchase an item from an auction site, never wire money for payment. There is no way you can get your money back if the auction is fraudulent. Always pay with a credit card so you can dispute fraudulent charges.

DON'T – Be a Victim of Bogus Scams. If an individual or website offers a deal that is too good to be true, it likely is. Scam sites may ask you to enter credit card information or directly transfer funds. These often appear in unsolicited emails. Even if the email appears to be from a legitimate retailer, go directly to their site to peruse deals instead of clicking email links.

DO – Always check credit card bills. Review credit card accounts regularly or sign up for your credit card to email or text you all purchases or authorizations. Put online receipts in a separate email folder, so you can easily crosscheck amounts.

DON'T – Provide excess information. A retailer often asks for your name, address, phone number and credit card number. However, you should never give out your driver's license number, social security number or bank routing numbers. If any site asks for this information, it is likely fraudulent.

hardeevillesc.gov
ISSUE 01 | MARCH 2023

WHAT DO WE DO?

The Information Technology Department builds reliable technology services while maintaining All compliance levels required with Cyber-Security at the forefront while bridging the gap between the end user and technology. The IT Department's main responsibilities include:

Life Cycle Management

- Budget and cost control
- Citizen/customer engagement experience
- Employee Training

Cyber Security

- CJIS compliance
- IT governance
- Infrastructure modernization
- Disaster recovery/continuity of operations
- Data governance: transparency, open data
- Business intelligence/analytics

Using the internet to purchase goods or services saves considerable time and effort – and also presents you with the widest choice. There are, however, risks associated with online shopping and you need to take care with what you are buying, from whom, and how you pay for your purchases.

THE RISKS

Using the internet to purchase goods or services saves considerable time and effort – and also presents you with the widest choice. There are, however, risks associated with online shopping and you need to take care with what you are buying, from whom, and how you pay for your purchases.

Fraud resulting from making payments over unsecured web pages. Fraud resulting from making payments using an unsecured Wi-Fi connection. Bogus online stores/shops – fake websites and email offers for goods and services that do not exist. Being offered tailored prices based on information gathered by the retailer about your online shopping habits and websites visited. Buying fake goods intentionally or unintentionally – finding they are of inferior quality and also possibly funding more serious crimes in the process. Losing your money when you make direct bank payments, only to find that the goods are inferior, or do not exist at all. Receiving goods or services which do not match the advertiser's description.

EYE ON IT Current Industry Trends

1. Artificial Intelligence and machine learning
2. Edge computing
3. 5G and other advanced wireless technologies
4. Internet of Things (IoT)
5. Virtual and augmented reality
6. Cybersecurity
7. Blockchain
8. Quantum computing
9. Robotic process automation
10. Biometric authentication and security

These are just a few examples, and it's possible that other emerging technologies could also rise to prominence in the coming years.

Hardeeville
SOUTH CAROLINA

hardeevillesc.gov
ISSUE 01 | MARCH 2023

TECH TALKS

HELPFUL LINKS

Password Manager

https://bitwarden.com

Data Breach

https://haveibeenpwned.com/

Hardeeville Hears & Helps

https://hardeevillesc.gov/2621/Hardeeville-Hears-and-Helps-Citizen-Port

THIS MONTH'S Q&A TECHNOLOGY TIPS: PASSWORD MANAGERS

Question: Are password managers safe?

Answer: Yes, password managers are safe to use, and that's a fact that not only the vast majority of cyber-security specialists agree with, but we do as well. After all, a **password manager uses advanced encryption to protect your credentials**, while without it, your passwords are accessible to anyone.

Question: Can a password manager be hacked?

Answer: Unfortunately, password managers have been hacked before. LastPass was recently breached in 2022, and One Login was hacked in 2017. However, neither breach revealed any customer passwords. Instead, hackers got access to the source code.